Greg Martin, Director of Technology
Administration Service Center
28W250 St. Charles Road
West Chicago, IL 6018
(630) 876-7800
www.benjamin25.org

Benjamin SCHOOL DISTRICT 25

TO: Board of Education
Dr. McGill
FROM: Greg Martin, Director of Technology
DATE: October 16, 2025
RE: Technology Report

Dear Board of Education Members,

The list below highlights a few of the updates and accomplishments over the past month:

- **Roster Server and ClassLink**
  Configured and deployed roster server and ClassLink integration. This ensures nightly automated, secure rostering of instructional resources, reduces manual account creation, and streamlines access for students and staff.

- **MBA PowerSchool Plugin Updates**
  Updated the MBA plugin configuration within PowerSchool to include new accounts and ensure accurate fee collection. This enhances reporting and alignment with the Business Office, resulting in more efficient financial tracking.

- **Deployed Read&Write Software**
  Deployed new Read&Write software across all student computers to support accessibility and learning equity. This rollout enhances reading and writing support for all students.

- **Securly Classroom Deployment**
  Configured and deployed Securly Classroom across the district, enabling teachers to monitor and guide student laptop use in real time. This strengthens classroom engagement and provides teachers with a tool to ensure students stay on task.

- **ClassLink Train-the-Trainer PD**
  Conducted professional development to train district staff in using ClassLink more effectively, ensuring long-term sustainability and local expertise.

Cybersecurity Awareness Month
Secure Insights: Your Monthly Cybersecurity Compass

- October 2025 Spotlight
  As the new school year began, distributed denial-of-service (DDoS) attacks against educational institutions doubled across the country, disrupting online learning platforms and network availability. These attacks overwhelm systems with massive amounts of malicious traffic, leaving students and teachers unable to access digital classrooms and critical resources. For schools statewide, the key lessons are clear: implement DDoS mitigation tools, build network redundancy with multiple connections, coordinate with ISPs and state agencies, and regularly test incident response playbooks.

- District Strengths and Protections
  Our district is well-prepared against these threats due to several proactive measures already in place:

    - Two separate Internet connections from different providers, each using distinct last-mile paths, to ensure redundancy and resilience.

    - Redundant links between our two schools with automatic failover, allowing network traffic to reroute seamlessly in case of an outage.

    - Extensive DDoS mitigation tools and automated services on one Internet connection, blocking malicious traffic before it reaches district networks.

    - A district firewall that provides an additional layer of protection, detecting and blocking malicious traffic at the perimeter.

Together, these safeguards position the district strongly to withstand external cyber threats and maintain continuity of learning.